DUMPSARENA

Associate - Networking Version 2.0?(DCA)

EMC DEA-5TT2

Version Demo

Total Demo Questions: 8

Total Premium Questions: 89

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Networking Fundamentals	25
Topic 2, Ethernet Switching	30
Topic 3, IP Routing	16
Topic 4, Network Services	12
Topic 5, Network Security	3
Topic 6, Network Management	3
Total	89

QUESTION NO: 1

Which protocol is used by a network device to resolve an IPv4 address to a MAC address on the local network?

A. Address Resolution Protocol (ARP)

B. Domain Name System (DNS)

C. Dynamic Host Configuration Protocol (DHCP)

D. Internet Control Message Protocol (ICMP)

ANSWER: A

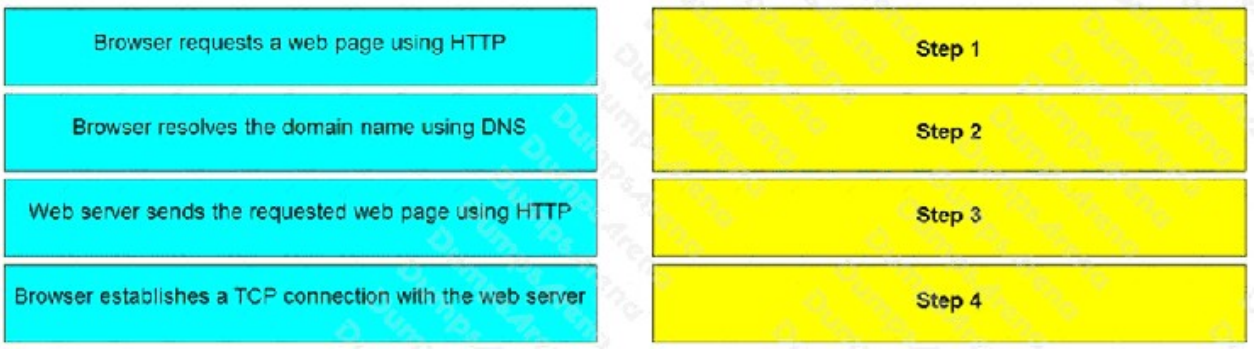
Explanation:

Address Resolution Protocol (ARP) is correct. Before sending an IPv4 packet across an Ethernet network, a host or router must know the destination MAC address to place in the Ethernet frame. For a local destination, the sender uses ARP to request the MAC address associated with the destination IPv4 address.

For an off-subnet destination, the sender uses ARP to resolve the MAC address of its default gateway rather than the remote host. ARP replies are commonly stored in an ARP cache for a period of time to avoid repeated requests. ARP operation is specified in RFC 826.

QUESTION NO: 2 - (SIMULATION)

What is the correct sequence of steps when a web browser accesses a web server?



ANSWER: See the explanation for the answer

Explanation:

The correct sequence is:

DNS first obtains the server IP address. The browser then creates the TCP transport connection before sending the HTTP request. The server returns the requested HTTP content over that connection.

QUESTION NO: 3

What is the usable host address range for the subnet 172.16.50.128/26?

A. 172.16.50.128 through 172.16.50.191

B. 172.16.50.129 through 172.16.50.190

C. 172.16.50.130 through 172.16.50.191

D. 172.16.50.129 through 172.16.50.254

ANSWER: B

Explanation:

172.16.50.129 through 172.16.50.190 is correct. A `/26` prefix uses the subnet mask `255.255.255.192`, which creates blocks of 64 addresses in the final octet. The subnet beginning at 172.16.50.128 spans addresses 172.16.50.128 through 172.16.50.191.

The first address, 172.16.50.128, is the network address and the final address, 172.16.50.191, is the directed broadcast address. The remaining 62 addresses, from 172.16.50.129 through 172.16.50.190, are assignable to hosts. CIDR addressing is described in RFC 4632.

QUESTION NO: 4

If a packet is sent to an IPv6 address and many devices receive the packet, what is this type of traffic?

A. Multicast

B. Broadcast

C. Anycast

D. Unicast

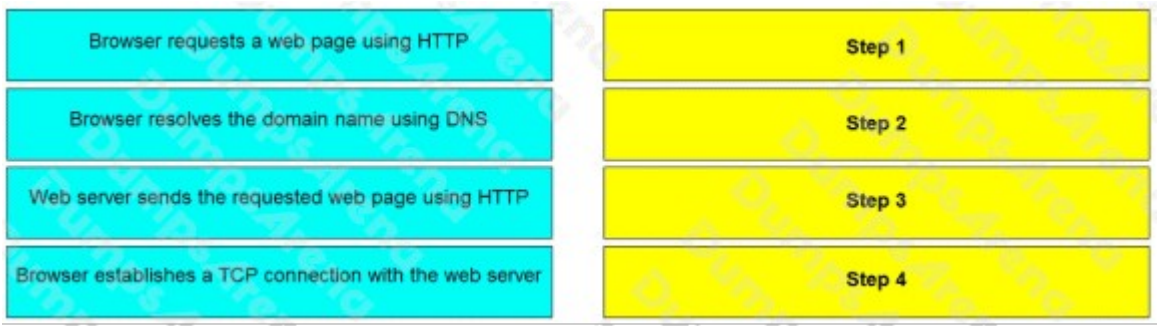
ANSWER: A

Explanation:

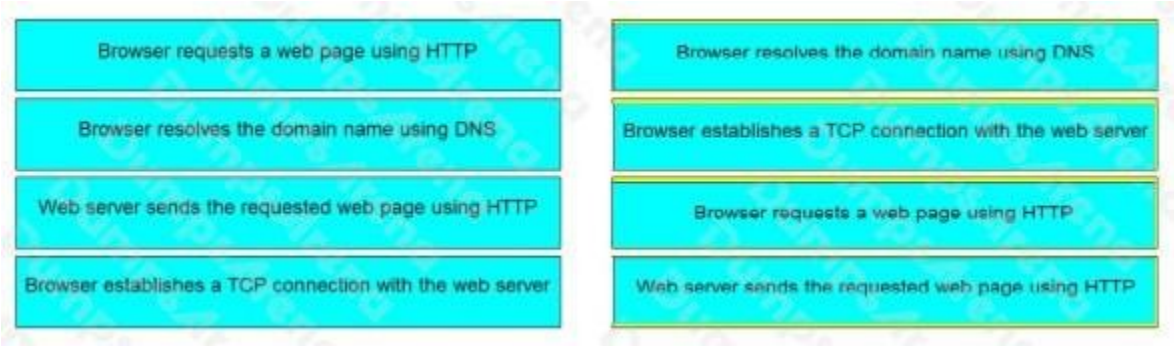
Multicast is the correct traffic type because IPv6 multicast delivers a packet from one sender to every interface that has joined the specified multicast group. A multicast destination identifies a group of receivers rather than one individual interface, allowing a sender to reach multiple interested devices efficiently with a single packet transmission. IPv6 multicast addresses use the `FF00::/8` prefix. For example, nodes use multicast for functions such as neighbor discovery and router discovery, where relevant devices on a link need to receive the same communication. IPv6 deliberately does not use the traditional broadcast mechanism used in IPv4; multicast serves the one-to-many communication role in IPv6. The IPv6 addressing architecture defines multicast as an identifier for a group of interfaces, with a packet sent to such an address delivered to all interfaces identified by that address. See the IETF IPv6 addressing specification in RFC 4291 and the IPv6 multicast overview in RFC 3306.

QUESTION NO: 5 - (DRAG DROP)

What is the correct sequence of steps when a web browser accesses a web server?



ANSWER:



Explanation:

When a user enters a web address, the browser first needs to determine where the named server is located on the network. It resolves the domain name using DNS, which translates the human-readable hostname into an IP address that can be used for network communication. DNS is therefore the first required action because the browser needs an address for the web server before it can initiate a connection. The Internet Engineering Task Force describes DNS terminology and operation in RFC 1034.

After obtaining the destination IP address, the browser establishes a TCP connection with the web server. TCP supplies the reliable, connection-oriented transport service traditionally used by HTTP, including connection setup before application data is exchanged. The TCP connection process is defined by the IETF in RFC 9293. Once that transport connection is available, the browser can request a web page using HTTP. This HTTP request identifies the resource the browser wants and carries any relevant request headers.

Finally, the web server sends the requested web page using HTTP. The response carries an HTTP status and the page content or other requested representation, allowing the browser to render the result for the user. HTTP's request/response semantics are specified in RFC 9110. Thus, the displayed placement correctly follows the dependency chain from name resolution, to reliable transport establishment, to the browser's request, and then to the server's response.

QUESTION NO: 6

Which route type is added to the routing table by a routing protocol?

A. Default route

B. Dynamic

C. Static

D. Directly connected

ANSWER: B

Explanation:

Dynamic is correct. A dynamic route is learned automatically through the operation of a routing protocol, such as OSPF, RIP, EIGRP, or BGP. The routing protocol exchanges reachability information with neighboring routers, evaluates the received paths according to its protocol-specific metrics and policies, and installs selected routes into the device's routing table. Dynamic routing allows the network to adapt when topology or link-state changes occur: when a preferred path becomes unavailable, the protocol can converge and select an alternate learned path where one is available. Routing-table entries commonly identify both the source routing protocol and the route's administrative preference or distance, helping the router choose between paths learned from different sources. This automatic learning and maintenance is the defining behavior of a dynamic route. Cisco's routing overview describes dynamic routing as routes that are learned by routing protocols and updated as network conditions change. For foundational IP-routing terminology and forwarding behavior, see Cisco IOS IP Routing Configuration Guide and RFC 1812: Requirements for IP Version 4 Routers.

QUESTION NO: 7

What is the default OSPF "hello interval"?

A. 5 seconds

B. 10 seconds

C. 15 seconds

D. 30 seconds

ANSWER: B

Explanation:

The correct answer is **10 seconds**. On the common OSPF network types used for Ethernet LANs and point-to-point links, OSPF routers send Hello packets every 10 seconds by default. These packets discover neighboring OSPF routers and maintain established neighbor adjacencies. Each router must use compatible Hello-related parameters on a shared segment for an adjacency to form, including the Hello interval and the dead interval. With the standard 10-second Hello timer, the default dead interval is typically 40 seconds, meaning a router normally declares a neighbor unavailable after four missed Hello intervals.

OSPF timer defaults are network-type dependent, so the 10-second value should be understood as the normal default for broadcast and point-to-point OSPF operation—the context generally intended when an exam question does not specify a network type. Administrators can tune these timers when faster failure detection is required, but the settings must remain consistent among adjacent routers. Cisco's OSPF configuration documentation lists the default Hello interval for broadcast and point-to-point network types as 10 seconds, while the OSPF protocol specification defines the Hello mechanism used to establish and maintain neighbor relationships. See Cisco IOS OSPF Configuration Guide and RFC 2328: OSPF Version 2.

QUESTION NO: 8

How many total addresses for network, broadcast, and host are provided with the subnet mask 255.255.255.240?

A. 8

B. 16

C. 24

D. 48

ANSWER: B

Explanation:

16 is correct. The subnet mask 255.255.255.240 has 28 network bits: the first three octets contribute 24 bits, and the final octet, 240, is binary 11110000, contributing four additional network bits. This is therefore a /28 IPv4 prefix. A /28 leaves four bits for addressing within each subnet. The number of total addresses in an IPv4 subnet is calculated as 2 raised to the number of remaining host bits, so 2^4 equals 16 total addresses. This total includes one network address, one broadcast address, and 14 addresses that can normally be assigned to hosts. For example, a subnet beginning at 192.168.1.0/28 spans 192.168.1.0 through 192.168.1.15: .0 is the network address, .15 is the broadcast address, and .1 through .14 are usable host addresses. The question explicitly asks for the total addresses provided for network, broadcast, and host purposes, rather than only usable host addresses. Cisco's IPv4 subnetting overview describes how prefix length determines the number of host bits and addresses: Cisco: IP Addressing and Subnetting for New Users. IPv4 address and prefix notation are also defined in RFC 4632.